Risk Reporter User Manual

Risk Reporter for PCI
ACR 2 Solutions

Table of Contents

1 Introduction

Risk Reporter (RR) is an automated system designed to simplify the process of creating and updating risk assessments. Risk assessment is the initial step required by most information security regulations, , including the Payment Card Industry Data Security Standard (PCI DSS), the Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and other state, federal, and international information security standards.

This RISK ASSESSMENT – PCI version is designed around the protocols created by the PCI DSS and the United States National Institute of Standards and Technology (NIST). The PCI DSS mandates minimum standards of security from any organization that handles payment cards, while the NIST procedures are rapidly becoming a de-facto international standard. This widespread adoption is due to the security automation efforts of the US Department of Homeland Security under the Security Content Automation Program (SCAP).

Automation of information security processes is essential for both adequate security and regulatory compliance. There are over 30,000 known vulnerabilities listed in the National Vulnerability Database (NVD), with more than 10 new vulnerabilities added daily. It is no longer practical to rely on general knowledge and manual checklists to secure an information system.

1.1 Typographical Conventions

This document uses the following typographical conventions:

- Command and option names appear in **bold type** in definitions and examples.
- The names of directories, files, screens, and menus appear in “quotes”.
- User inputted data appears bolded inside **<angle brackets>**.
- Website addresses appear underlined.
- Hyperlinks appear underlined and in blue font.
- Notational usage information appears in indented and in *italic type*.

2 Risk Management History and Overview

Risk assessment is a process that was largely developed in the environmental industry in the 1970s and involves review of vulnerabilities, probability of damage, and the impact of damage. As the federal government and other regulators realized its enormous benefit of risk assessments, they mandated organizations in more industries to conduct them.

In 2004, Visa, MasterCard, American Express, and Discover combined resources to create a single PCI Data Security Standard (DSS) with the goal of helping organizations protect customer information, safeguard transactions, and conduct risk assessments to identify vulnerabilities. The risk assessment process is continual; details of the DSS requirements vary according to the size of the organization, but in each case three steps are required:

1. Risk Assessment
2. Safeguards Implementation based on the risk assessment
3. Vulnerability Assessment to measure the effectiveness of the Safeguard Implementation

As of June 2007, the DSS applies to every organization that processes payment card information, including merchants and third-party service providers that store, process, or transmit payment card data. Failure to comply with the Payment Card Industry security standards may result in heavy fines, restrictions, or permanent expulsion from card acceptance programs.

Other industries also developed standardized risk assessment requirements. In 2002, the NIST produced a simplified risk assessment for use with "sensitive but unclassified" information. These risk assessments are mandatory for organizations regulated under FISMA, and are recommended for those regulated by GLBA and the Health Insurance Portability and Accountability Act (HIPAA). Risk Reporter assessment scores are calculated using the PCI DSS Requirement questions, Compensating Control (NIST Safeguard) questions, and UTM/configuration scan data.

The risk management process continues to advance. Policy data and safeguards installations change at a slow rate, but network configurations may change daily and UTM data changes from minute to minute. Automated risk assessments, which automatically upload data from the UTM and network scans on a daily basis, are now possible. Policy changes may be added as they occur, creating the "near real-time" risk assessment that is the goal of NIST 800-39, the "flagship document of the NIST 800 series" (800-39, 42).

3 The Risk Reporter Assessment Process

Risk Reporter risk assessment software utilizes information from an organization's existing Unified Threat Management (UTM) device/Intrusion Prevention System (IPS), Anti-Virus (AV) program, and a detailed NIST policy questionnaire to produce a quantitative, NIST compliant risk assessment[AKS1].

Assessed risk categories include Environmental, Human Error, Malicious Insider, and Malicious Outsider. Per the NIST 800-30 requirements, risks categories are rated from 1 to 100.

3.1 Collecting the Data

To complete a risk assessment, you will need familiarity with and access to:

- The organization's Information Security Policy and Procedures
- Information about personnel with access to protected data
- The organization's most recent SCAP scan file

3.2 Accessing the RR Website

Browse to http://your_product_site[AKS2].net as shown in Figure 3.1. Enter the case-sensitive **Username** and **Password** (Serial Number) provided with the RR CD or in the welcome e-mail, then click the **Login** button.

> *Note: For enhanced security, risk assessment sessions will timeout after 24 minutes on a single screen.*

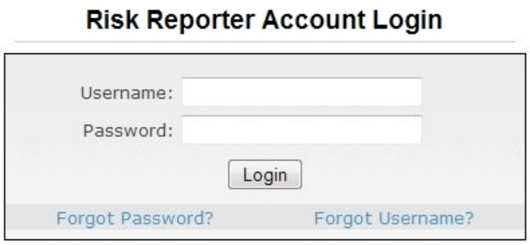
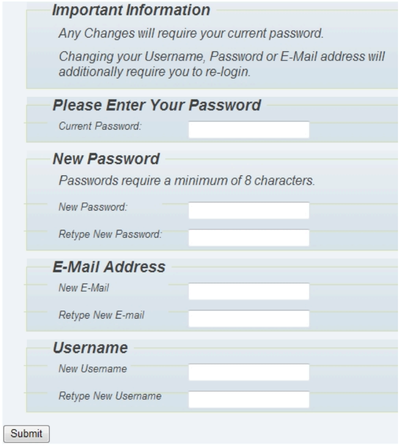


Figure 3.1 Login screen

Upon logging in, you will be directed to the **Account Settings** screen shown Figure 3.2. You must change your Username and Password before completing an assessment. Because login information may be e-mailed, it is not secure and cannot be used for data entry. You must also enter the email address at which you wish to receive the risk assessment reports.



Important Information

Any Changes will require your current password.

Changing your Username, Password or E-Mail address will additionally require you to re-login.

Please Enter Your Password

Current Password:

New Password

Passwords require a minimum of 8 characters.

New Password:

Retype New Password:

E-Mail Address

New E-Mail

Retype New E-mail

Username

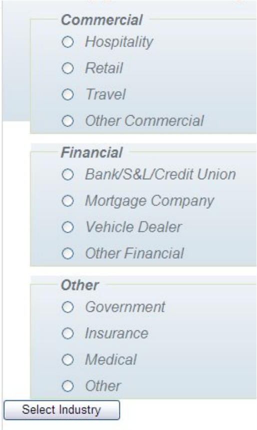
New Username

Retype New Username

Figure 3.2 Account Settings

After changing the account/verification information, you will need to login again, using the new information.

The next step in the account creation process is industry selection, shown in Figure 3.3. This information will indicate the typical regulatory scheme to be considered in the assessment. While the overall risk assessment process is similar for a variety of regulations, there are differences in the details.



Commercial

○ Hospitality

○ Retail

○ Travel

○ Other Commercial

Financial

○ Bank/S&L/Credit Union

○ Mortgage Company

○ Vehicle Dealer

○ Other Financial

Other

○ Government

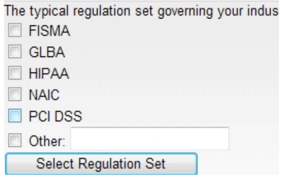
○ Insurance

○ Medical

○ Other

Figure 3.3 Industry Selection

After selecting your industry, you must select any additional regulations governing your organization’s risk assessment; verify that PCI DSS is selected.



The typical regulation set governing your indus

□ FISMA

□ GLBA

□ HIPAA

□ NAIC

□ PCI DSS

□ Other:

Figure 3.4 Regulation Selection

After selecting the regulatory environment, you will see the **Main Menu**, Figure 3.5.

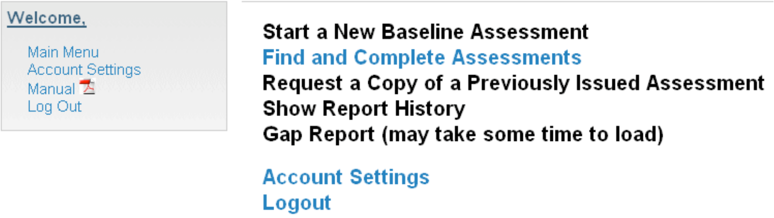
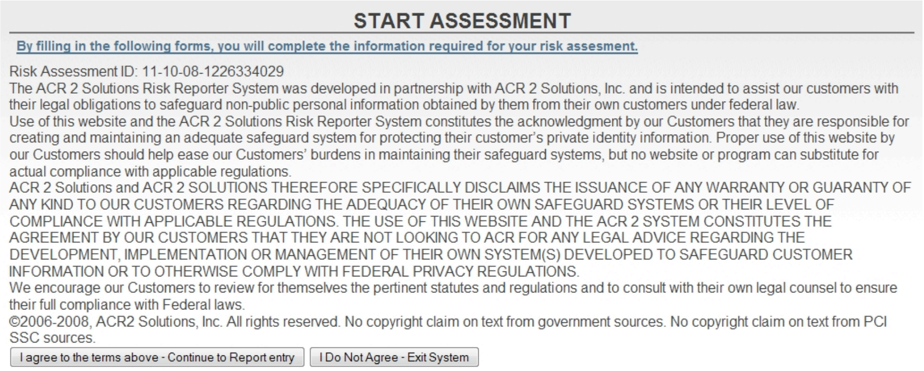

Welcome,
Main Menu
Account Settings
Manual
Log Out
Start a New Baseline Assessment
Find and Complete Assessments
Request a Copy of a Previously Issued Assessment
Show Report History
Gap Report (may take some time to load)
Account Settings
Logout

Figure 3.5 Main Menu

When you are ready to begin an assessment, return to the **Main Menu** and click the **Start a New Baseline Assessment** line. The Baseline is the first risk assessment of a calendar year; all updated assessments will be compared to this assessment.

Before you can enter data, you must read and accept the **Disclaimer**, shown in Figure 3.6. RR is a repackaging of PCI DSS and/or NIST protocols, and is offered in good faith, but control over data entry is the responsibility of users; no warranty is offered or possible.



START ASSESSMENT

By filling in the following forms, you will complete the information required for your risk assesment.

Risk Assessment ID: 11-10-08-1226334029

The ACR 2 Solutions Risk Reporter System was developed in partnership with ACR 2 Solutions, Inc. and is intended to assist our customers with their legal obligations to safeguard non-public personal information obtained by them from their own customers under federal law.

Use of this website and the ACR 2 Solutions Risk Reporter System constitutes the acknowledgment by our Customers that they are responsible for creating and maintaining an adequate safeguard system for protecting their customer's private identity information. Proper use of this website by our Customers should help ease our Customers' burdens in maintaining their safeguard systems, but no website or program can substitute for actual compliance with applicable regulations.

ACR 2 Solutions and ACR 2 SOLUTIONS THEREFORE SPECIFICALLY DISCLAIMS THE ISSUANCE OF ANY WARRANTY OR GUARANTY OF ANY KIND TO OUR CUSTOMERS REGARDING THE ADEQUACY OF THEIR OWN SAFEGUARD SYSTEMS OR THEIR LEVEL OF COMPLIANCE WITH APPLICABLE REGULATIONS. THE USE OF THIS WEBSITE AND THE ACR 2 SYSTEM CONSTITUTES THE AGREEMENT BY OUR CUSTOMERS THAT THEY ARE NOT LOOKING TO ACR FOR ANY LEGAL ADVICE REGARDING THE DEVELOPMENT, IMPLEMENTATION OR MANAGEMENT OF THEIR OWN SYSTEM(S) DEVELOPED TO SAFEGUARD CUSTOMER INFORMATION OR TO OTHERWISE COMPLY WITH FEDERAL PRIVACY REGULATIONS.

We encourage our Customers to review for themselves the pertinent statutes and regulations and to consult with their own legal counsel to ensure their full compliance with Federal laws.

©2006-2008, ACR2 Solutions, Inc. All rights reserved. No copyright claim on text from government sources. No copyright claim on text from PCI SSC sources.

I agree to the terms above - Continue to Report entry
I Do Not Agree - Exit System

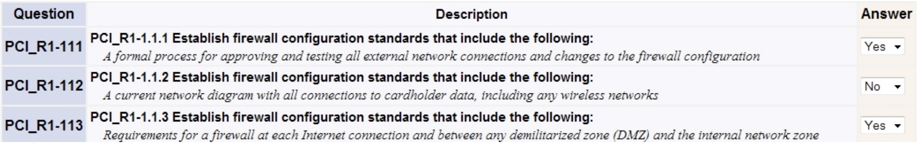
Figure 3.6 Disclaimer

Click the "**I agree"** button to bring up the first data entry screen.

3.3 Policy Questions

The first questions section of the risk assessment pertains to the 203 questions in the 12 PCI security Requirements. The second section is a series of potential compensating controls taken from the 170 Security Control questions contained in the NIST risk assessment (800-39) and minimum safeguards (800-53) protocols.

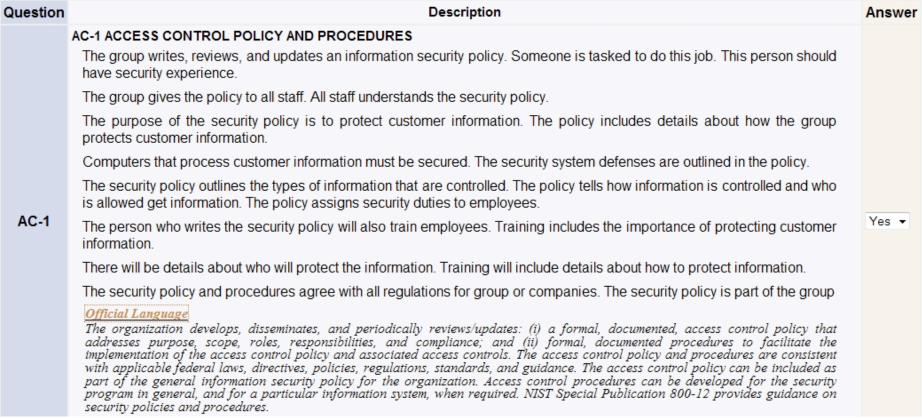
Answer each question by selecting the most appropriate choice from the pull-down menu. The options are **No** - the safeguard is not in place or functioning, **Yes** - the safeguard is in place and functioning, or **NA** - the safeguard does not apply at this location. The default answer for each question is No, the most conservative answer.



Question	Description	Answer
PCI_R1-111	**PCI_R1-1.1.1 Establish firewall configuration standards that include the following:** *A formal process for approving and testing all external network connections and changes to the firewall configuration*	Yes ▾
PCI_R1-112	**PCI_R1-1.1.2 Establish firewall configuration standards that include the following:** *A current network diagram with all connections to cardholder data, including any wireless networks*	No ▾
PCI_R1-113	**PCI_R1-1.1.3 Establish firewall configuration standards that include the following:** *Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone*	Yes ▾

Figure 3.7 Sample PCI Question

The language of the Compensating Controls is a plain English paraphrase of the original wording. To view the original wording for any NIST safeguard, click **Official Language** at the end of the paraphrase. The paraphrase and official language for question AC-1 is shown below.



Question	Description	Answer
AC-1	**AC-1 ACCESS CONTROL POLICY AND PROCEDURES** The group writes, reviews, and updates an information security policy. Someone is tasked to do this job. This person should have security experience. The group gives the policy to all staff. All staff understands the security policy. The purpose of the security policy is to protect customer information. The policy includes details about how the group protects customer information. Computers that process customer information must be secured. The security system defenses are outlined in the policy. The security policy outlines the types of information that are controlled. The policy tells how information is controlled and who is allowed get information. The policy assigns security duties to employees. The person who writes the security policy will also train employees. Training includes the importance of protecting customer information. There will be details about who will protect the information. Training will include details about how to protect information. The security policy and procedures agree with all regulations for group or companies. The security policy is part of the group *Official Language* *The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. The access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.*	Yes ▾

Figure 3.8 Sample Compensating Control Question

After answering the last question in a section, click the **Save and Continue** button to update the next data section. This is a secure transmission and may take up to a minute to load; do not press the button more than once. To update a different data section, use the navigation buttons or the pull down menu.

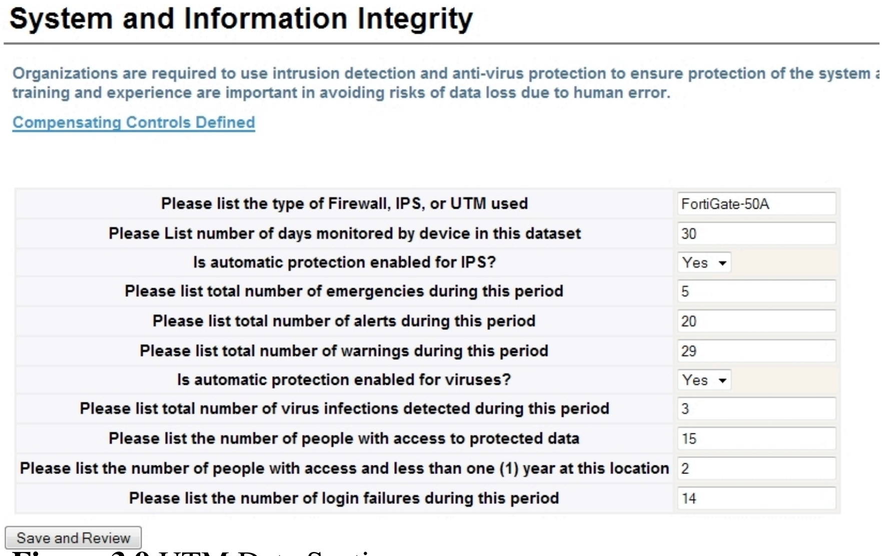
> *Note: Using any navigation tool will result in the loss of data inputted into the section. To save changes, click the* ***Save and Continue*** *button.*

Depending upon your familiarity with your organization's Information Security Policy and Procedures, completing a risk assessment may take as few as three hours. However, assessments do not need to be completed in a single sitting. To interrupt a data session, use the **Log Out** line in the menu box of each data screen. When you log back in, an option to **Find and Complete Assessments** will appear in the Main Menu.

Selecting an incomplete assessment brings up the Review screen shown in Figure 3.11; click any section to load that data entry page. This selection is also a secure transmission and may take up to a minute to load.

3.4 UTM Data

This data section is different from the others. As shown in Figure 3.9, it requires numerical, UTM/IPS, and AV data.



System and Information Integrity

Organizations are required to use intrusion detection and anti-virus protection to ensure protection of the system a
training and experience are important in avoiding risks of data loss due to human error.

Compensating Controls Defined

Please list the type of Firewall, IPS, or UTM used	FortiGate-50A
Please List number of days monitored by device in this dataset	30
Is automatic protection enabled for IPS?	Yes ▾
Please list total number of emergencies during this period	5
Please list total number of alerts during this period	20
Please list total number of warnings during this period	29
Is automatic protection enabled for viruses?	Yes ▾
Please list total number of virus infections detected during this period	3
Please list the number of people with access to protected data	15
Please list the number of people with access and less than one (1) year at this location	2
Please list the number of login failures during this period	14

Figure 3.9 UTM Data Section

3.5 XCCDF Upload

This data section requires you to upload the organization's most recent SCAP scan.

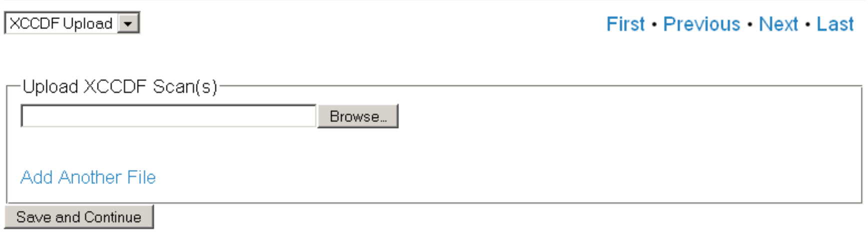
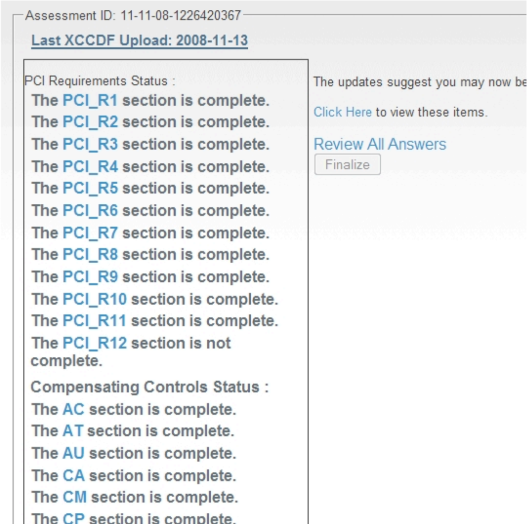


Figure 3.10 XCCDF Upload Section

3.6 Data Review

The final section is the Review Screen. Once all of the sections have been updated, the **Finalize** button becomes active, as shown in Figure 3.11, and a Baseline Report can be generated.



Assessment ID: 11-11-08-1226420367

Last XCCDF Upload: 2008-11-13

PCI Requirements Status :

The PCI_R1 section is complete.
The PCI_R2 section is complete.
The PCI_R3 section is complete.
The PCI_R4 section is complete.
The PCI_R5 section is complete.
The PCI_R6 section is complete.
The PCI_R7 section is complete.
The PCI_R8 section is complete.
The PCI_R9 section is complete.
The PCI_R10 section is complete.
The PCI_R11 section is complete.
The PCI_R12 section is not complete.

Compensating Controls Status :

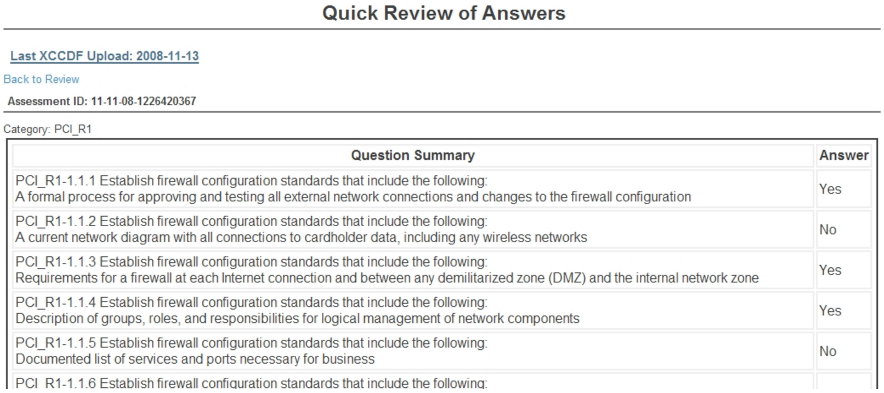
The AC section is complete.
The AT section is complete.
The AU section is complete.
The CA section is complete.
The CM section is complete.
The CP section is complete.

The updates suggest you may now be

Click Here to view these items.

Figure 3.11 Review Section

There are several ways to review your answers before submitting an assessment. Click a blue section link or use the pull-down menu to navigate back to the desired control section, or click the **Review All Answers** line above the Finalize button. As shown in Figure 3.12, this will bring up a summary of your answers.



Quick Review of Answers

Last XCCDF Upload: 2008-11-13

Assessment ID: 11-11-08-1226420367

Category: PCI_R1

Question Summary	Answer
PCI_R1-1.1.1 Establish firewall configuration standards that include the following: A formal process for approving and testing all external network connections and changes to the firewall configuration	Yes
PCI_R1-1.1.2 Establish firewall configuration standards that include the following: A current network diagram with all connections to cardholder data, including any wireless networks	No
PCI_R1-1.1.3 Establish firewall configuration standards that include the following: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Yes
PCI_R1-1.1.4 Establish firewall configuration standards that include the following: Description of groups, roles, and responsibilities for logical management of network components	Yes
PCI_R1-1.1.5 Establish firewall configuration standards that include the following: Documented list of services and ports necessary for business	No
PCI_R1-1.1.6 Establish firewall configuration standards that include the following:	

Figure 3.12 Quick Review

3.7 The Results

RR reports are designed to help organizations efficiently prioritize and organize safeguards which must be put into place or updated. The risk assessment data will generate two reports, a Baseline Report and a Chart Report. These locked reports are e-mailed to the account that was specified during the account creation process, and require your account password to open. Two additional reports, the PCI Inventory Report and the PCI Gap Report accessible from the Main Menu, are also generated.

> *Note: Access to e-mailed reports requires the installation of Adobe® Acrobat Reader® Version 6.0 or newer.*

See Appendix A for report samples.

1. **baseline.pdf** - a numerical scoring of risks to information security and availability. Risks are defined as threat source/vulnerability combinations, and are divided into 30 risk categories based on the NIST protocols. Risks range from E1, wind/roof damage, to MO8, malicious outsider/internal controls.

   The Baseline Report is the first report generated in the year and cannot be altered; future assessments will generate an Update Report (**update.pdf**). When compared to update reports, the Baseline enables you to determine the degree of change in the organization's risk scores.

2. **chart.pdf** - a graphical, color coded representation of the baseline or update risk scores. Red/yellow/green coding indicates high, medium, and low risk status, respectively.

3. **PCI Inventory Report** - an overview listing the answers to each question in the most recent risk assessment. Information from all data entry sections is included.

4. **PCI Gap Report** - a detailed list of missing or underperforming safeguards, which have negatively affected the most recent risk assessment. Holding the cursor over each safeguard gives more information about the threat source and affected vulnerability.

These reports enable user to create an Action Plan for the organization. Low, Medium, and High likelihoods of adverse events are scored at 0.1, 0.5, or 1.0, respectively. In the same manner, Low, Medium, and High impacts are scored at 10, 50, and 100 respectively. A risk score, from 1 (low) to 100 (high) is calculated by multiplying the likelihood score and the impact score.

According to NIST standards, risks scores >50 require immediate action, risks scores from 10 to 50 need to be scheduled for management, and risks <10 can be monitored without further action.

4 Applying the Risk Assessment

Compliance is a continuously moving target; conducting a risk assessment is only part of the risk management process. Regulated firms are required to

1. Assess risks
2. Install Safeguards
3. Test Safeguard effectiveness
4. Re-assess risks

Data from a network scan (800-30 section 3.1), IPS data, Antivirus data (Section 3.3), and policy data are input into the Risk Engine. This creates the Results Documentation (Section 3.9) and recommendations for change.

The changes in Controls are implemented and the changes added to the risk engine, along with updated Scan, IPS, and AV data. This cycle can be done as often as daily, with reports on demand.

The risk management process is an ongoing cycle that will continue as long as the organization remains in operation.

4.1 Creating an Action Plan

Following the review and acceptance of these risk reports by management, it is necessary to create an action plan. The plan should prioritize the needed safeguards in order to increase or maintain compliance with information security regulations.

You may find the PCI Inventory Report and PCI Gap report (accessible from the Main Menu) useful for quickly determining which areas are in need of improvement. The Inventory Report provides a summary of every answer inputted for the most recent assessment, while the Gap Report shows which safeguards negatively affected the assessment. Once you have identified the needed safeguards, they can be listed using data from the Deficiency Report Key in Appendix B.

In most cases, the Action Plan will address upgrades in order of cost and convenience. Many changes are inexpensive and demonstrate progress to regulators without major cost, but other changes may require capital planning before being phased in.

For example, safeguard SI-5, Security Alerts and Advisories, is easy to update. A number of free websites can fill this need, including several government sites such as Computer Emergency Readiness Team (CERT). On the other hand, CP-2, which requires the creation of a NIST compliant Contingency Plan, can be a major effort.

Once the action plan for red risks is in place, implement a similar program for yellow risks. Under NIST guidelines, risks in the yellow range need to be "scheduled for remediation". Again, the fastest and least expensive rule of prioritization is a prudent use of limited corporate resources. On a weekly basis, as new safeguards are implemented, the risk assessment can be updated with new reports. At a minimum, a monthly reassessment of risk is recommended, and should be placed in the appropriate portion of the organization’s Information Security Plan notebook.

Compliance regulators do not expect organizations to be perfectly secure. However, "reasonable and appropriate" progress is not only expected, but required. Periodic, quantitative risk assessment reports can provide a low cost means of documenting the organization's compliance level.

4.2 Creating an Update Report

Creating an update report is easy. Login to an account that has had a baseline report issued within the last 12 months and select **Find and Complete Assessments**, as shown in Figure 4.1.

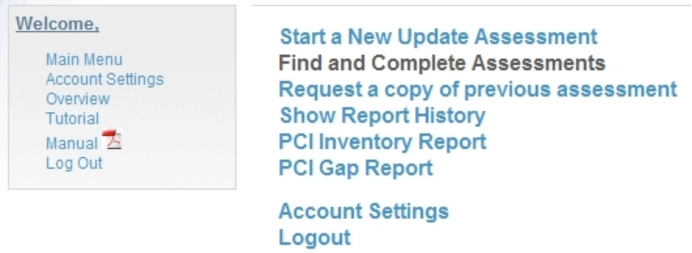
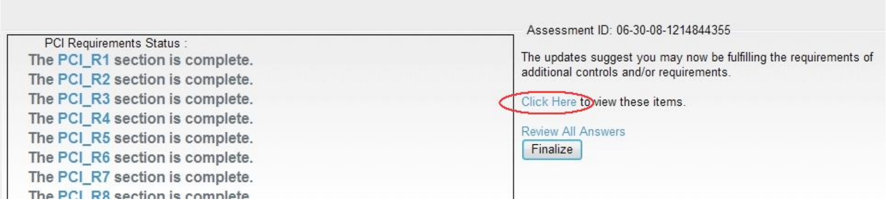


Figure 4.1 Main Menu

As with the Baseline report, data entry sections begin after the disclaimer is accepted; use the pull down menu to change the assessment as needed. Once you have made any known changes, check the **Review** page to determine if additional input is required. From time to time the PCI DSS and NIST update the controls. When that occurs, you will see **Questions not reviewed**. You must answer these questions before an update report can be issued.

Additionally, because the security questions are interrelated, RR software analyzes the changes made to data sections and recommends additional changes via a notification message on the review screen. To view the suggested changes, select **Click Here** as shown in Figure 4.2.



PCI Requirements Status :
The PCI_R1 section is complete.
The PCI_R2 section is complete.
The PCI_R3 section is complete.
The PCI_R4 section is complete.
The PCI_R5 section is complete.
The PCI_R6 section is complete.
The PCI_R7 section is complete.
The PCI_R8 section is complete.

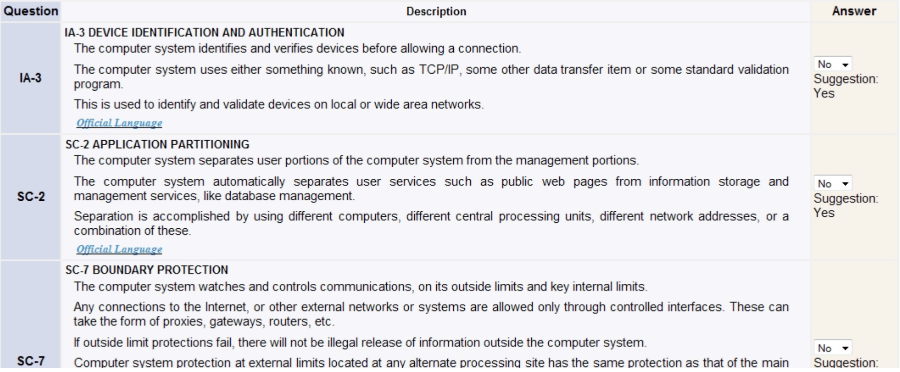
Assessment ID: 06-30-08-1214844355

The updates suggest you may now be fulfilling the requirements of additional controls and/or requirements.

Click Here to view these items.

Figure 4.2 Suggested Answers Notification

Clicking the link will provide additional information about affected questions, as shown in Figure 4.3.

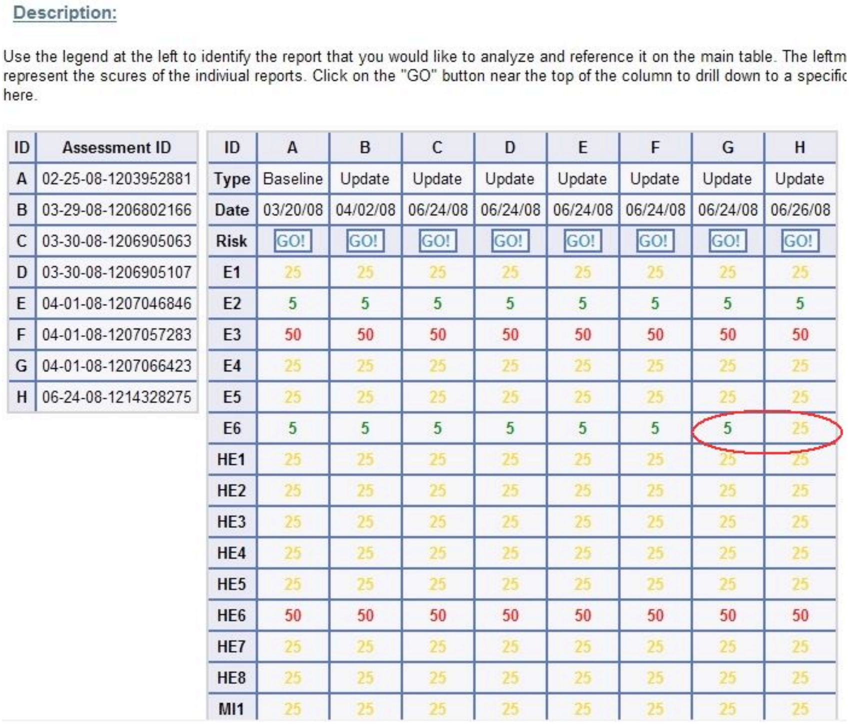


Question	Description	Answer
IA-3	IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION The computer system identifies and verifies devices before allowing a connection. The computer system uses either something known, such as TCP/IP, some other data transfer item or some standard validation program. This is used to identify and validate devices on local or wide area networks. *Official Language*	No ▾ Suggestion: Yes
SC-2	SC-2 APPLICATION PARTITIONING The computer system separates user portions of the computer system from the management portions. The computer system automatically separates user services such as public web pages from information storage and management services, like database management. Separation is accomplished by using different computers, different central processing units, different network addresses, or a combination of these. *Official Language*	No ▾ Suggestion: Yes
SC-7	SC-7 BOUNDARY PROTECTION The computer system watches and controls communications, on its outside limits and key internal limits. Any connections to the Internet, or other external networks or systems are allowed only through controlled interfaces. These can take the form of proxies, gateways, routers, etc. If outside limit protections fail, there will not be illegal release of information outside the computer system. Computer system protection at external limits located at any alternate processing site has the same protection as that of the main	No ▾ Suggestion:

Figure 4.3 Suggested Changes

After you have generated a Baseline report, the Main Menu option to **Show Report History** will become active. This feature is most useful after you have generated multiple reports; it allows you to determine what input changed between assessments, and thus, which policies and procedures, scan, or upload changes affected the risk score.

Figure 4.4 shows an increased risk to E6.



Description:

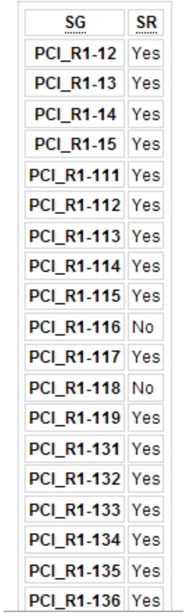
Use the legend at the left to identify the report that you would like to analyze and reference it on the main table. The leftm
represent the scures of the indiviual reports. Click on the "GO" button near the top of the column to drill down to a specific
here.

ID	Assessment ID
A	02-25-08-1203952881
B	03-29-08-1206802166
C	03-30-08-1206905063
D	03-30-08-1206905107
E	04-01-08-1207046846
F	04-01-08-1207057283
G	04-01-08-1207066423
H	06-24-08-1214328275

ID	A	B	C	D	E	F	G	H
Type	Baseline	Update	Update	Update	Update	Update	Update	Update
Date	03/20/08	04/02/08	06/24/08	06/24/08	06/24/08	06/24/08	06/24/08	06/26/08
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	25	25	25	25	25	25	25	25
E2	5	5	5	5	5	5	5	5
E3	50	50	50	50	50	50	50	50
E4	25	25	25	25	25	25	25	25
E5	25	25	25	25	25	25	25	25
E6	5	5	5	5	5	5	5	25
HE1	25	25	25	25	25	25	25	25
HE2	25	25	25	25	25	25	25	25
HE3	25	25	25	25	25	25	25	25
HE4	25	25	25	25	25	25	25	25
HE5	25	25	25	25	25	25	25	25
HE6	50	50	50	50	50	50	50	50
HE7	25	25	25	25	25	25	25	25
HE8	25	25	25	25	25	25	25	25
MI1	25	25	25	25	25	25	25	25

Figure 4.4 Multi-Report Overview

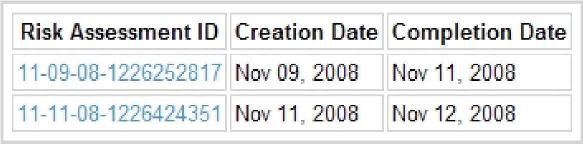
Click **GO!** to view the data submitted for each assessment. As shown in Figure 4.5, this screen gives a summary of the data submitted for each report.



SG	SR
PCI_R1-12	Yes
PCI_R1-13	Yes
PCI_R1-14	Yes
PCI_R1-15	Yes
PCI_R1-111	Yes
PCI_R1-112	Yes
PCI_R1-113	Yes
PCI_R1-114	Yes
PCI_R1-115	Yes
PCI_R1-116	No
PCI_R1-117	Yes
PCI_R1-118	No
PCI_R1-119	Yes
PCI_R1-131	Yes
PCI_R1-132	Yes
PCI_R1-133	Yes
PCI_R1-134	Yes
PCI_R1-135	Yes
PCI_R1-136	Yes

Figure 4.5 Report Detail

In order to compare differences between assessments more easily, you may also wish to view the reports that were generated from an earlier assessment. From the Main Menu, select **Request a Copy of a Previous Assessment**. As shown in Figure 4.6, this will allow you to select an assessment and receive, via locked, PDF reports, the reports it generated.



Risk Assessment ID	Creation Date	Completion Date
11-09-08-1226252817	Nov 09, 2008	Nov 11, 2008
11-11-08-1226424351	Nov 11, 2008	Nov 12, 2008

Figure 4.6 Request a Report Copy

5 Contact Information

Thank you for your interest in Risk Reporter. For general information, contact Sales Rep:

E-mail: Sales@acr2solutions.com
Phone: 1. 678-261-8181

5.1 Technical Support

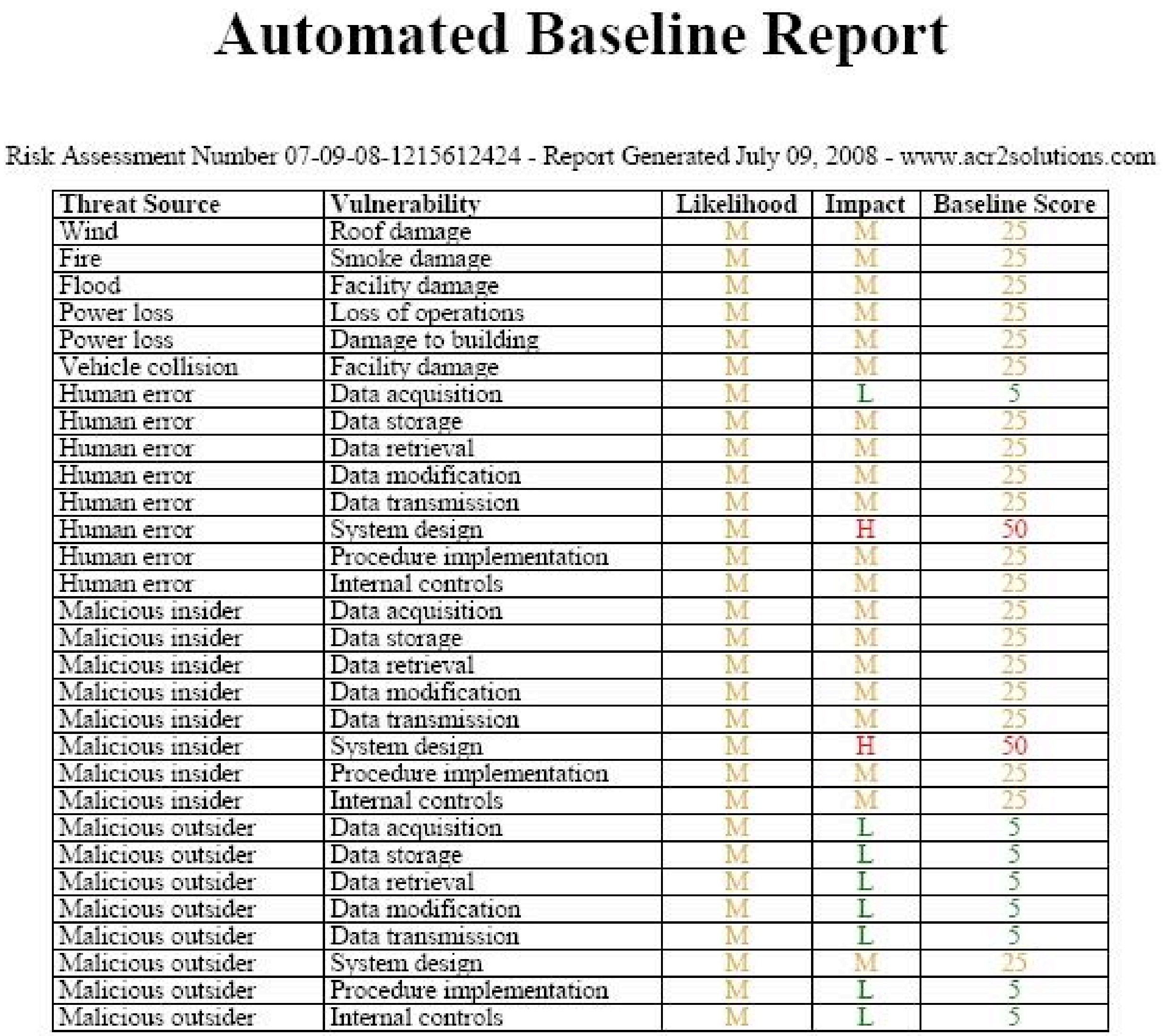
Technical support for RR is available 8 hours a day, 5 days a week. Please review the appropriate section of the manual before contacting technical support.

If the problem persists email support@acr2solutions.com

When contacting support, please have the following information available:

- The version of Risk Reporter software you are using
- The computer's browser and operating system version

Appendix A – Sample Reports

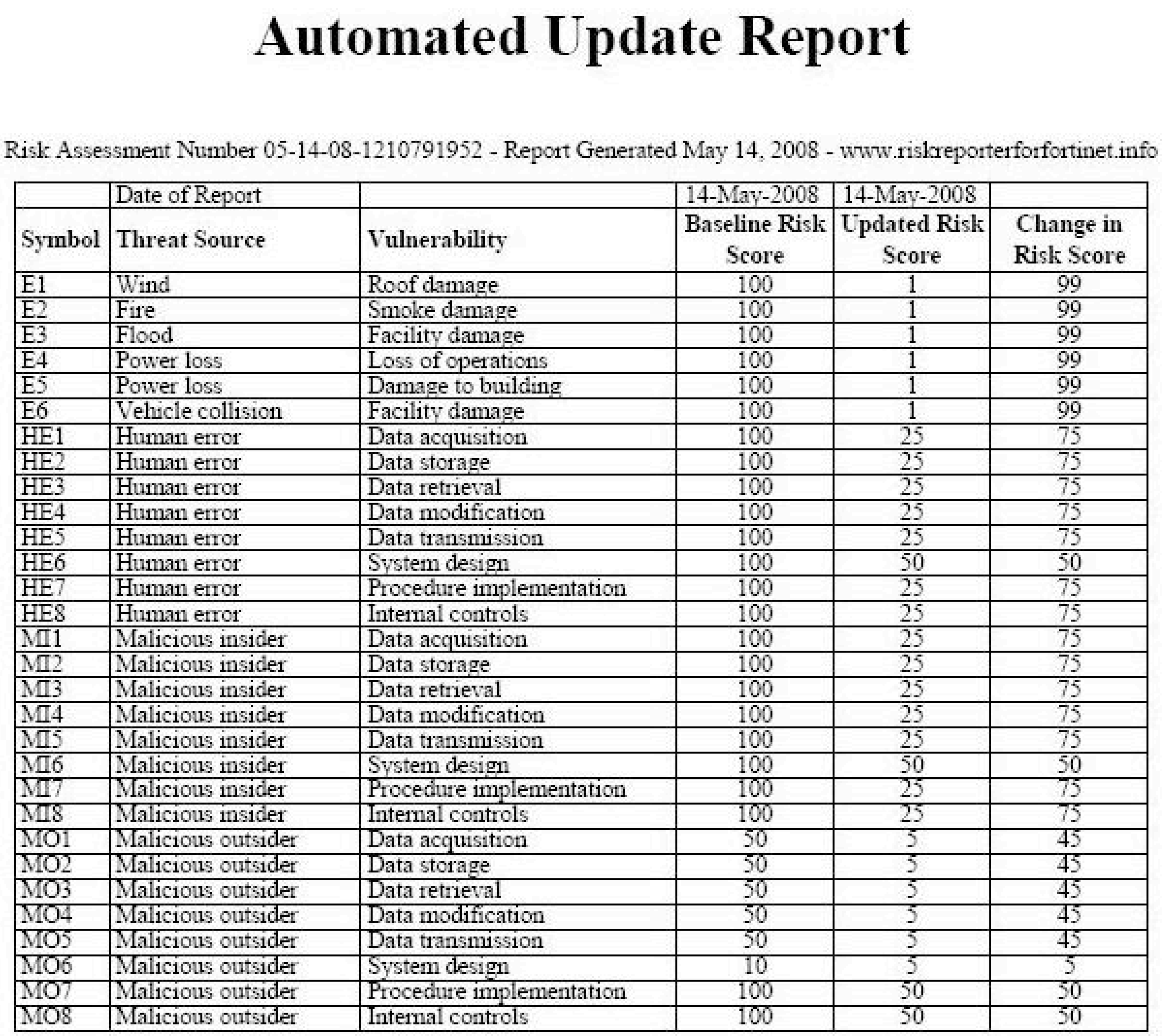


Automated Baseline Report

Risk Assessment Number 07-09-08-1215612424 - Report Generated July 09, 2008 - www.acr2solutions.com

Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
Wind	Roof damage	M	M	25
Fire	Smoke damage	M	M	25
Flood	Facility damage	M	M	25
Power loss	Loss of operations	M	M	25
Power loss	Damage to building	M	M	25
Vehicle collision	Facility damage	M	M	25
Human error	Data acquisition	M	L	5
Human error	Data storage	M	M	25
Human error	Data retrieval	M	M	25
Human error	Data modification	M	M	25
Human error	Data transmission	M	M	25
Human error	System design	M	H	50
Human error	Procedure implementation	M	M	25
Human error	Internal controls	M	M	25
Malicious insider	Data acquisition	M	M	25
Malicious insider	Data storage	M	M	25
Malicious insider	Data retrieval	M	M	25
Malicious insider	Data modification	M	M	25
Malicious insider	Data transmission	M	M	25
Malicious insider	System design	M	H	50
Malicious insider	Procedure implementation	M	M	25
Malicious insider	Internal controls	M	M	25
Malicious outsider	Data acquisition	M	L	5
Malicious outsider	Data storage	M	L	5
Malicious outsider	Data retrieval	M	L	5
Malicious outsider	Data modification	M	L	5
Malicious outsider	Data transmission	M	L	5
Malicious outsider	System design	M	M	25
Malicious outsider	Procedure implementation	M	L	5
Malicious outsider	Internal controls	M	L	5

Baseline Report



Automated Update Report

Risk Assessment Number 05-14-08-1210791952 - Report Generated May 14, 2008 - www.riskreporterforfortinet.info

	Date of Report		14-May-2008	14-May-2008	
Symbol	**Threat Source**	**Vulnerability**	**Baseline Risk Score**	**Updated Risk Score**	**Change in Risk Score**
E1	Wind	Roof damage	100	1	99
E2	Fire	Smoke damage	100	1	99
E3	Flood	Facility damage	100	1	99
E4	Power loss	Loss of operations	100	1	99
E5	Power loss	Damage to building	100	1	99
E6	Vehicle collision	Facility damage	100	1	99
HE1	Human error	Data acquisition	100	25	75
HE2	Human error	Data storage	100	25	75
HE3	Human error	Data retrieval	100	25	75
HE4	Human error	Data modification	100	25	75
HE5	Human error	Data transmission	100	25	75
HE6	Human error	System design	100	50	50
HE7	Human error	Procedure implementation	100	25	75
HE8	Human error	Internal controls	100	25	75
MI1	Malicious insider	Data acquisition	100	25	75
MI2	Malicious insider	Data storage	100	25	75
MI3	Malicious insider	Data retrieval	100	25	75
MI4	Malicious insider	Data modification	100	25	75
MI5	Malicious insider	Data transmission	100	25	75
MI6	Malicious insider	System design	100	50	50
MI7	Malicious insider	Procedure implementation	100	25	75
MI8	Malicious insider	Internal controls	100	25	75
MO1	Malicious outsider	Data acquisition	50	5	45
MO2	Malicious outsider	Data storage	50	5	45
MO3	Malicious outsider	Data retrieval	50	5	45
MO4	Malicious outsider	Data modification	50	5	45
MO5	Malicious outsider	Data transmission	50	5	45
MO6	Malicious outsider	System design	10	5	5
MO7	Malicious outsider	Procedure implementation	100	50	50
MO8	Malicious outsider	Internal controls	100	50	50

Update Report

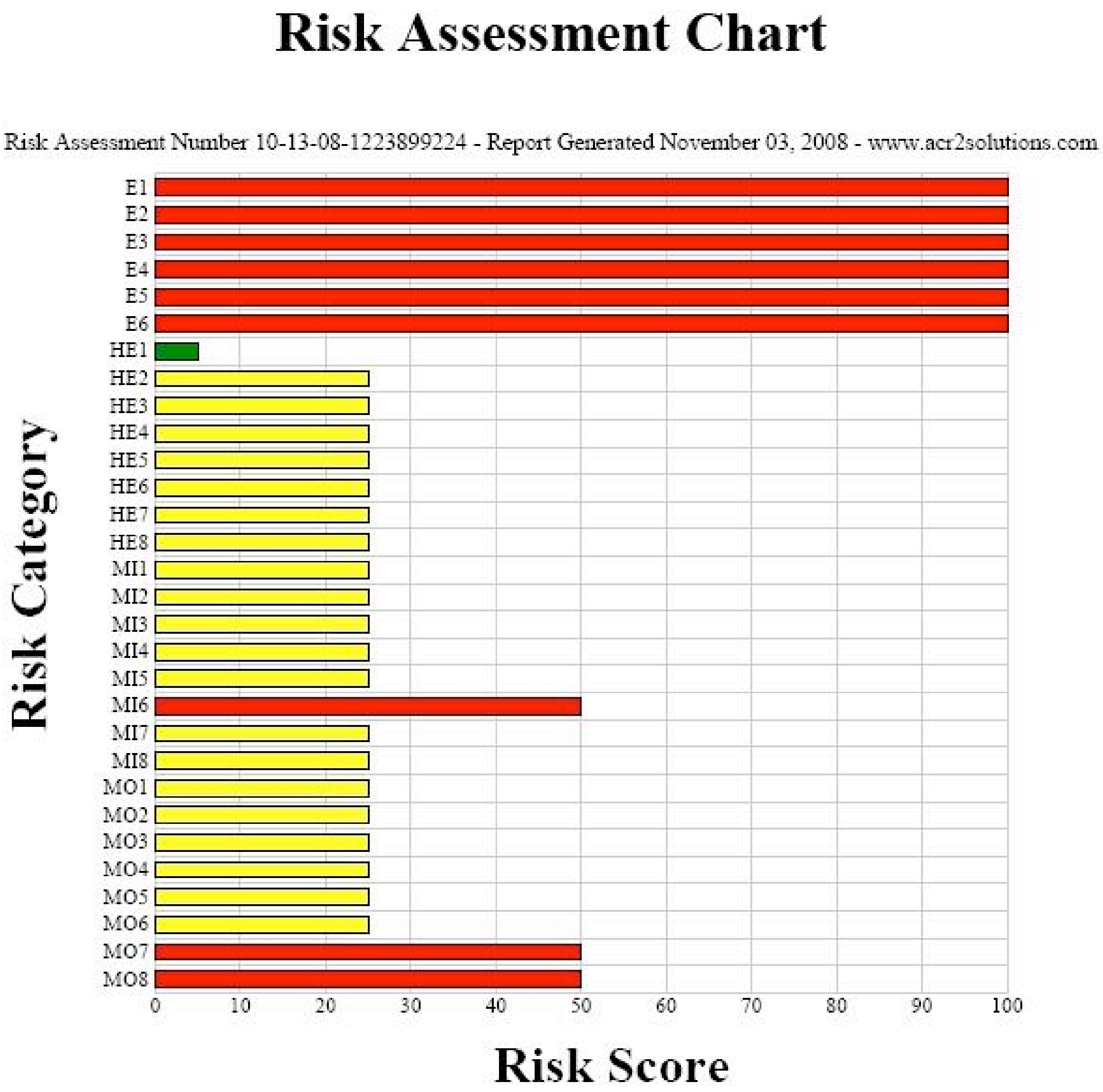
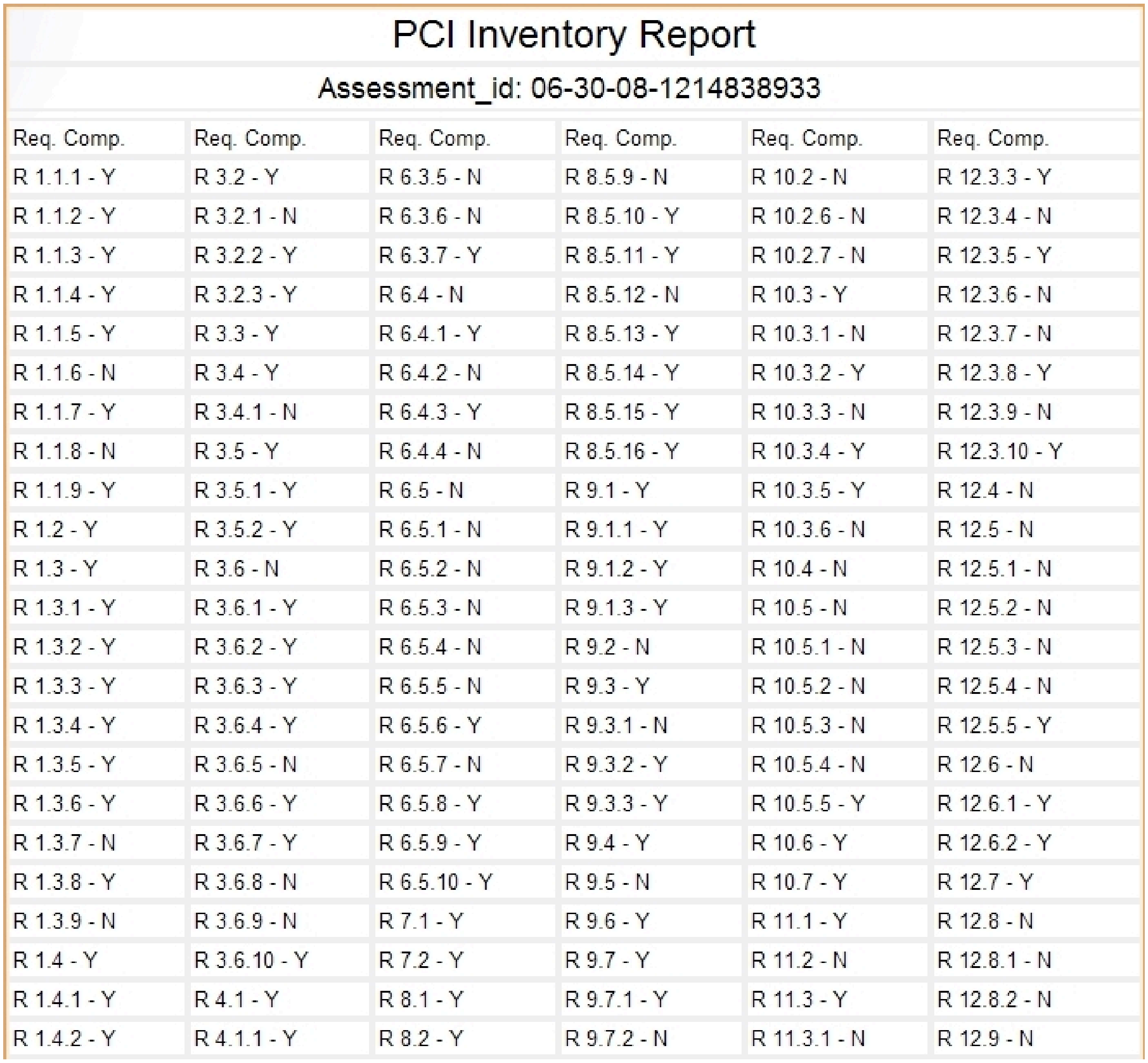


Chart Report

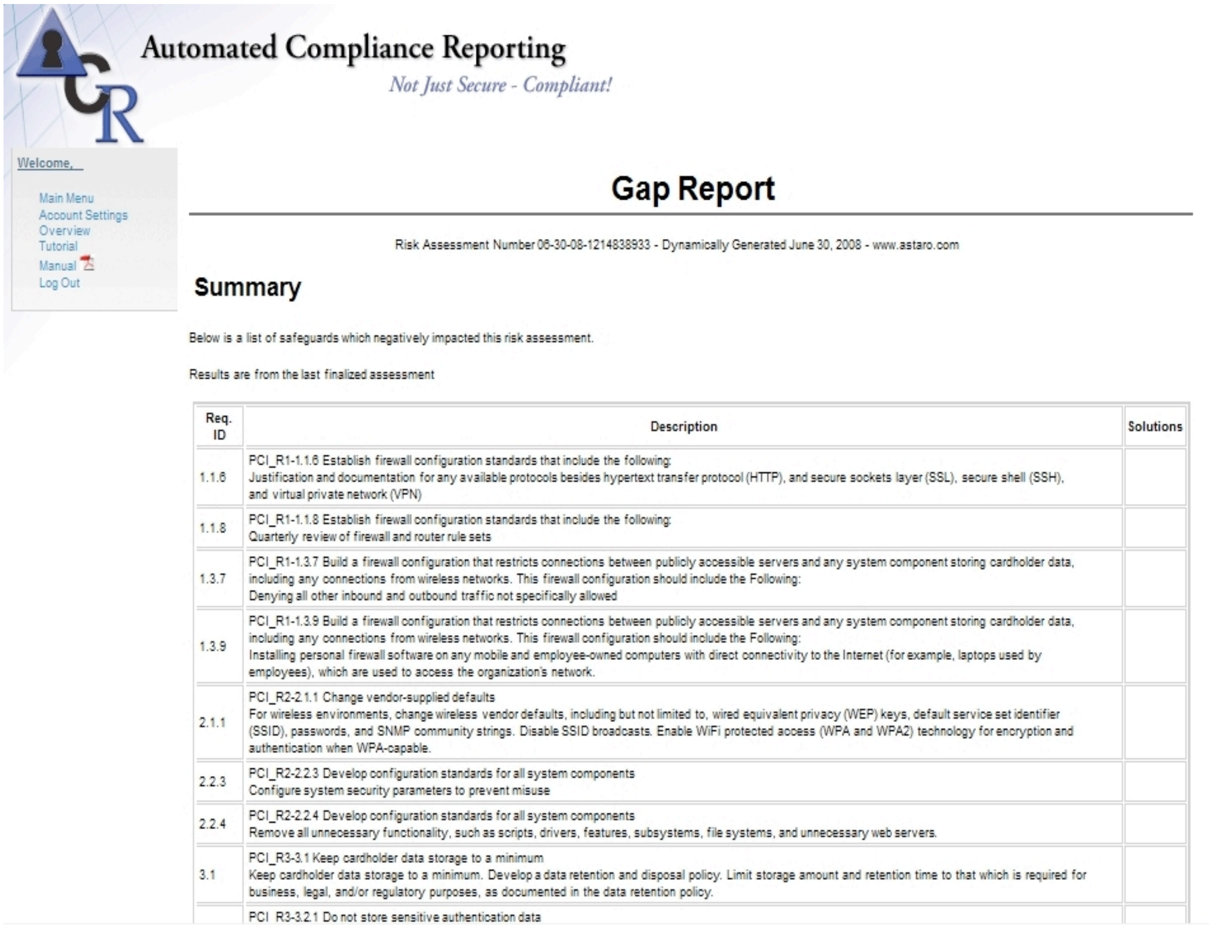


PCI Inventory Report

Assessment_id: 06-30-08-1214838933

Req. Comp.	Req. Comp.	Req. Comp.	Req. Comp.	Req. Comp.	Req. Comp.
R 1.1.1 - Y	R 3.2 - Y	R 6.3.5 - N	R 8.5.9 - N	R 10.2 - N	R 12.3.3 - Y
R 1.1.2 - Y	R 3.2.1 - N	R 6.3.6 - N	R 8.5.10 - Y	R 10.2.6 - N	R 12.3.4 - N
R 1.1.3 - Y	R 3.2.2 - Y	R 6.3.7 - Y	R 8.5.11 - Y	R 10.2.7 - N	R 12.3.5 - Y
R 1.1.4 - Y	R 3.2.3 - Y	R 6.4 - N	R 8.5.12 - N	R 10.3 - Y	R 12.3.6 - N
R 1.1.5 - Y	R 3.3 - Y	R 6.4.1 - Y	R 8.5.13 - Y	R 10.3.1 - N	R 12.3.7 - N
R 1.1.6 - N	R 3.4 - Y	R 6.4.2 - N	R 8.5.14 - Y	R 10.3.2 - Y	R 12.3.8 - Y
R 1.1.7 - Y	R 3.4.1 - N	R 6.4.3 - Y	R 8.5.15 - Y	R 10.3.3 - N	R 12.3.9 - N
R 1.1.8 - N	R 3.5 - Y	R 6.4.4 - N	R 8.5.16 - Y	R 10.3.4 - Y	R 12.3.10 - Y
R 1.1.9 - Y	R 3.5.1 - Y	R 6.5 - N	R 9.1 - Y	R 10.3.5 - Y	R 12.4 - N
R 1.2 - Y	R 3.5.2 - Y	R 6.5.1 - N	R 9.1.1 - Y	R 10.3.6 - N	R 12.5 - N
R 1.3 - Y	R 3.6 - N	R 6.5.2 - N	R 9.1.2 - Y	R 10.4 - N	R 12.5.1 - N
R 1.3.1 - Y	R 3.6.1 - Y	R 6.5.3 - N	R 9.1.3 - Y	R 10.5 - N	R 12.5.2 - N
R 1.3.2 - Y	R 3.6.2 - Y	R 6.5.4 - N	R 9.2 - N	R 10.5.1 - N	R 12.5.3 - N
R 1.3.3 - Y	R 3.6.3 - Y	R 6.5.5 - N	R 9.3 - Y	R 10.5.2 - N	R 12.5.4 - N
R 1.3.4 - Y	R 3.6.4 - Y	R 6.5.6 - Y	R 9.3.1 - N	R 10.5.3 - N	R 12.5.5 - Y
R 1.3.5 - Y	R 3.6.5 - N	R 6.5.7 - N	R 9.3.2 - Y	R 10.5.4 - N	R 12.6 - N
R 1.3.6 - Y	R 3.6.6 - Y	R 6.5.8 - Y	R 9.3.3 - Y	R 10.5.5 - Y	R 12.6.1 - Y
R 1.3.7 - N	R 3.6.7 - Y	R 6.5.9 - Y	R 9.4 - Y	R 10.6 - Y	R 12.6.2 - Y
R 1.3.8 - Y	R 3.6.8 - N	R 6.5.10 - Y	R 9.5 - N	R 10.7 - Y	R 12.7 - Y
R 1.3.9 - N	R 3.6.9 - N	R 7.1 - Y	R 9.6 - Y	R 11.1 - Y	R 12.8 - N
R 1.4 - Y	R 3.6.10 - Y	R 7.2 - Y	R 9.7 - Y	R 11.2 - N	R 12.8.1 - N
R 1.4.1 - Y	R 4.1 - Y	R 8.1 - Y	R 9.7.1 - Y	R 11.3 - Y	R 12.8.2 - N
R 1.4.2 - Y	R 4.1.1 - Y	R 8.2 - Y	R 9.7.2 - N	R 11.3.1 - N	R 12.9 - N

Inventory Report



Gap Report

Risk Assessment Number 06-30-08-1214838933 - Dynamically Generated June 30, 2008 - www.astaro.com

Summary

Below is a list of safeguards which negatively impacted this risk assessment.

Results are from the last finalized assessment

Req. ID	Description	Solutions
1.1.6	PCI_R1-1.1.6 Establish firewall configuration standards that include the following: Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	
1.1.8	PCI_R1-1.1.8 Establish firewall configuration standards that include the following: Quarterly review of firewall and router rule sets	
1.3.7	PCI_R1-1.3.7 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the Following: Denying all other inbound and outbound traffic not specifically allowed	
1.3.9	PCI_R1-1.3.9 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the Following: Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	
2.1.1	PCI_R2-2.1.1 Change vendor-supplied defaults For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.	
2.2.3	PCI_R2-2.2.3 Develop configuration standards for all system components Configure system security parameters to prevent misuse	
2.2.4	PCI_R2-2.2.4 Develop configuration standards for all system components Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	
3.1	PCI_R3-3.1 Keep cardholder data storage to a minimum Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	
	PCI R3-3.2.1 Do not store sensitive authentication data	

Gap Report

Appendix B – Deficiency Report Key

Label	Threat Source	Vulnerability
E1	Wind	Roof Damage
E2	Fire	Smoke Damage
E3	Flood	Facility Damage
E4	Power Loss	Loss of Operations
E5	Power Loss	Damage to Building
E6	Vehicle Collision	Facility Damage
HE1	Human Error	Data Acquisition
HE2	Human Error	Data Storage
HE3	Human Error	Data Retrieval
HE4	Human Error	Data Modification
HE5	Human Error	Data Transmission
HE6	Human Error	System Design
HE7	Human Error	Procedure Implementation
HE8	Human Error	Internal Controls
MI1	Malicious Insider	Data Acquisition
MI2	Malicious Insider	Data Storage
MI3	Malicious Insider	Data Retrieval
MI4	Malicious Insider	Data Modification
MI5	Malicious Insider	Data Transmission
MI6	Malicious Insider	System Design
MI7	Malicious Insider	Procedure Implementation
MI8	Malicious Insider	Internal Controls
MO1	Malicious Outsider	Data Acquisition
MO2	Malicious Outsider	Data Storage
MO3	Malicious Outsider	Data Retrieval
MO4	Malicious Outsider	Data Modification
MO5	Malicious Outsider	Data Transmission
MO6	Malicious Outsider	System Design
MO7	Malicious Outsider	Procedure Implementation
MO8	Malicious Outsider	Internal Controls

Appendix C – Glossary

Term	Meaning
Action Plan	A plan to prioritize and upgrade system safeguards to maintain or increase compliance.
Administrative Account	An account with administrative permissions to one or more systems on a network.
Administrative Scan Account	Administrators may create these accounts specifically for the purpose of conducting ThreatGuard Scans. More complex networks may require the creation of several accounts.
Baseline Report	The first risk assessment of a calendar year. This contains a numerical scoring of risks to information security and availability. All future risk assessments will be compared to the Baseline report.
Chart Report	A graphical, color coded representation of the baseline or update risk scores.
Compensating Control	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.
Compliance Officer	The individual responsible for conducting the risk assessment.
Deficiency Report	A cross listing of missing or underperforming safeguards.
Federal Enterprise Architecture (FEA)	A business-based framework for government-wide improvement developed by the OMB. It is intended to ease efforts to move the federal government toward becoming citizen-centered, results-oriented, and market-based.
Gap Report	A chart indicating “gaps” in security compliance. This report specifies which questions/factors negatively impacted the Risk Assessment score.
Group	CEOs, Managers, etc. who are responsible for maintaining security compliance.
Hub	A device used to connect multiple networking cables together to make them act as one unit.
Hyperlink (link)	Clickable text or graphics that direct the user to another document (typically a website) or to another place within the same document.
Internal Network	The client’s network.
Intrusion Detection System (IDS)	Software or hardware that detects attacks on a computer or network, but is incapable of stopping data damage or retrieval.

Intrusion Prevention System (IPS)	Software or hardware that is capable of real-time prevention of an attack on a computer or network.
Isolated Network	Internal ACR 2 network.
Magnus Navigator	The client application that is used to configure and manage the Secutor Magnus server.
Network Administrator	The individual responsible for installing the system. This individual manages the local area communications network within an organization and, traditionally, is responsible for the configuration, maintenance, day-to-day operations, and installation of infrastructure components.
Network Address Translation	The process of passing network traffic through a router that re-writes the source and/or destination IP addresses.
Risk	The likelihood that a vulnerability will be exploited, modified by the impact of the exploitation.
Risk Score Change	Risk Scores may change due to changes in the safeguards an organization uses or because of safeguard performance.
Router	A computer that is configured to route and forward information.
Software as a Service (SaaS)	A sales model whereby access to the software application is hosted by the seller and the user is provided access via the Internet.
Status Report	A compilation of the current status of the safeguards for the information system.
Substantial Compliance	Several aspects of security compliance are covered in each question. If a majority of aspects are in place, the group is considered to be in substantial compliance and may answer “Yes” to the question.
System Logging (Syslog)	The transmittal of event messages and alerts across an IP network. Messages are sent by the operating system or application to report the current status of a process.
Unified Threat Management (UTM)	UTM is used to describe network firewalls that have many features in one box, including e-mail spam filtering, anti-virus capability, an intrusion detection (or prevention) system (IDS or IPS), and World Wide Web content filtering, along with the traditional activities of a firewall.
Update Report	Any report made after the Baseline report. Determines the degree of increase or decrease in compliance compared to the baseline. Update risk assessments are required after system changes.
Vulnerability	Areas where security is weak and is at risk of being exploited.